УДК 343.982

В. Е. Козлов
доцент кафедры тактико-специальной подготовки
факультета милиции Академии МВД Республики Беларусь,
кандидат юридических наук, доцент

ОБ ОТДЕЛЬНЫХ АСПЕКТАХ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

В узком смысле противодействие компьютерной (высокотехнологичной) преступности нами рассматривается как деятельность правоохранительных органов, направленная против компьютерных преступлений (в т. ч. их выявление, предупреждение, профилактика, пресечение, раскрытие и расследование), осуществляемая в целях установления контроля над ней. Важное место в искомом процессе занимает взаимодействие правоохранительных органов с операторами электросвязи (далее – ЭС), интернет-провайдерами. Его основой являются положения статьи 43 Закона Республики Беларусь «Об электросвязи» от 19 июля 2005 г. № 45-З, согласно которой операторы ЭС в ходе осуществления оперативно-розыскной деятельности (далее – ОРД) органами, определенными соответствующим законом, обязаны:

предоставлять в случаях и порядке, установленных законодательными актами, информацию о пользователях услуг ЭС и об оказанных им услугах ЭС, а также иную информацию, необходимую для выполнения возложенных на эти органы задач;

в случаях и порядке, установленных законодательными актами, оказывать содействие в проведении оперативно-розыскных мероприятий (далее – ОРМ) и предоставлять возможность их проведения на сетях ЭС, принимать меры по защите сведений об организационных и тактических приемах проведения ОРМ;

обеспечивать в случаях и порядке, определенных законодательными актами, доступ к базам данных, автоматизированным системам оператора ЭС;

обеспечивать выполнение обязательных для соблюдения требований технических нормативных правовых актов в области технического нормирования и стандартизации, а также иных требований, установленных законодательством к сетям и средствам ЭС, при проведении ОРМ.

Порядок предоставления информации регламентируется Указом Президента Республики Беларусь № 129 от 3 марта 2010 г. «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность» в

случаях оказания содействия в проведении ОРМ и создании условий для их проведения на сетях ЭС, а также обеспечения доступа к базам данных (далее – БД), автоматизированным системам операторов, предоставления информации о пользователях услуг ЭС и об оказанных им услугах ЭС, а также к иной информации, необходимой для выполнения задач, возложенных на уполномоченные органы.

По требованию уполномоченных подразделений оператор ЭС обязан обеспечить безвозмездный круглосуточный удаленный доступ к БД об абонентах с использованием технических средств уполномоченных органов, к БД об оказанных абонентам услугах ЭС, автоматизированным системам операторов, а также передавать уполномоченным подразделениям в режиме реального времени информацию обо всех оказанных абонентам услугах ЭС. Перечень сведений, содержащихся в БД оператора ЭС, определен как для физических, так и для юридических лиц. Для физических лиц это абонентский номер, фамилия, имя, отчество, адрес абонента или адрес установки оконечного абонентского устройства, данные, позволяющие идентифицировать абонента или его оконечное устройство, а для абонентов сети сотовой подвижной ЭС – также реквизиты документа, удостоверяющего личность.

Названная информация, зафиксированная на материальных носителях с реквизитами, позволяющими ее идентифицировать, хранится пять лет.

В процессе совершенствования национального законодательства Республики Беларусь по вопросам противодействия преступности возникла необходимость детализации требований к информации, хранящейся у операторов ЭС, оказывающих услуги по доступу в сеть Интернет. Они сформулированы в постановлении Министерства связи и информатизации Республики Беларусь № 6 от 18 февраля 2015 г. «Об утверждении Инструкции о порядке формирования и хранения сведений о посещаемых пользователями интернет-услуг информационных ресурсах». Постановлением определена дефиниция понятия «интернет-ресурс», под которой понимается интернет-сайт, страница интернет-сайта, веб-портал, форум, блог, чат, приложение для мобильного устройства и другие ресурсы, имеющие подключение к глобальной компьютерной сети Интернет. Поставщики интернет-услуг обязаны с использованием собственного аппаратно-программного комплекса формировать и хранить актуальные сведения о посещаемых пользователями интернет-услуг (ПИУ) интернет-ресурсах, которые включают в себя сведения о ПИУ, и обо всех услугах ЭС, им активированных, а также дату, время начала и окончания соединений, внутренний и внешний IP-адреса и порты оконечного абонентского устройства, доменное имя или IP-адрес и порт посещаемого ПИУ интернет-ресурса, объем переданных и принятых данных.

Кроме того, в развитие положений Указа №129 детализирована документированная информация, подлежащая хранению в течение одного года. Например, для физических лиц:

номер и дата заключения договора на оказание услуг ЭС, фамилия, имя, отчество, адрес пользователя или адрес установки оконечного абонентского устройства;

данные, позволяющие идентифицировать ПИУ или его оконечное абонентское устройство, MAC-адрес или идентификационный номер оконечного абонентского устройства ПИУ сотовой подвижной ЭС;

для абонентов сети сотовой подвижной ЭС – реквизиты документа, удостоверяющего личность.

Следует отметить, что приведенные правовые и организационные меры доказали свою эффективность во многих странах. Однако существуют и определенные ограничения по использованию их результатов в предупреждении, выявлении, раскрытии и расследовании компьютерных («высокотехнологичных») преступлений, которые детерминированы возрастающей квалификацией субъектов совершения преступлений, заключающейся в использовании возможностей Интернета для сокрытия преступной деятельности. Анализ семиуровневой модели ISO/OSI, а также доступных ПИУ технологий к таковым позволяет отнести:

proxy-серверы (Opera, Google и т.д), а также VPN-сервисы и серверы «анонимизации»;

технологии децентрализованных сетей (Invisible Internet Project – I2P), а также гибридных анонимных сетей (The Onion Router – Tor).

Использование указанных технологий существенно затрудняет процесс идентификации ПИУ на уровне «ПИУ–интернет–ресурс».

Изложенное позволяет сделать следующие выводы.

1. Принимаемые организационно-правовые меры эффективны и своевременны лишь по отношению к ПИУ, использующим интернет в преступных целях без технологий сокрытия и «анонимизации».

2. Лавинообразное повышение «криминальной квалификации» ПИУ, совершающих рассматриваемые преступления, детерминирует совершенствование разработанных и внедренных методик «компьютерной» и «аналитической» разведок, осуществляемых в ходе ОРД оперативными подразделениями правоохранительных органов, а также использование их результатов в уголовном процессе.

3. Совершенствование названных методик противодействия в сложившихся условиях кадрового и учебно-методического обеспечения возможно в ведомственных учреждениях образования правоохранительных органов страны путем совершенствования тематических планов и (или) внедрения специализированных учебных курсов.